

SEGURANÇA OFENSIVA

AFINAL, O QUE É ISTO?

#> QUEM SOU EU



MATEUS BUOGO

FORMACAO

- R E D E S D E COMPUTADORES
- MBA ADMINISTRACAO DE TI
- M E S T R A N D O E M ADMINISTRACAO

PROFISSIONAL

- ANALISTA DE SEGURANCA
- PROFESSOR

CONTATO

MBUOGORSE@GMAIL.COM

MATEUSBUOGO@LETS HACK.COM.BR



LET'S HACK

[HTTPS://LETS HACK.COM.BR](https://lets hack.com.br)



#> SEGURANCA OFENSIVA



ONDE TUDO
COMECOU?



#> SEGURANCA OFENSIVA



NOME **BONITO** PARA
UTILIZAR TECNICAS **DE**
HACKING PARA IDENTIFICAR
VULNERABILIDADE EM
SISTEMAS CORPORATIVOS.



#> ESTAMOS EXPOSTOS?



O DESAFIO DA CIBERSEGURANÇA NA SAÚDE

PARA CLAUDIO BANNWART, COUNTRY MANAGER DA CHECK POINT NO BRASIL, OS BAIXOS NÍVEIS DE SEGURANÇA QUE OS HOSPITAIS APRESENTAM FACILITAM O ACESSO A UM ENORME VOLUME DE INFORMAÇÕES SENSÍVEIS, O QUE POR SUA VEZ PERMITE A OBTENÇÃO DE ELEVADOS PROVEITOS FINANCEIROS POR PARTE DOS ATACANTES.

PORTAL SECURITY REPORT - 25/09/2019



#> ESTAMOS EXPOSTOS?



DISPOSITIVOS DE
SAUDE Podem
ACARRETAR RISCOS
PARA A SEGURANCA
CIBERNETICA

AS PRINCIPAIS AMEACAS CIBERNETICAS QUE ATINGEM OS DISPOSITIVOS DE SAUDE Podem SER DIVIDIDAS EM TRES TIPOS: AQUELAS QUE VIOLAM A PRIVACIDADE DOS DADOS, AS QUE COMPROMETEM A INTEGRIDADE DESTES E AS QUE ATACAM SUA DISPONIBILIDADE.

PORTAL SECURITY REPORT - 18/01/2019



#> ESTAMOS EXPOSTOS?



VIOLACOES DE DADOS
COMPROMETERAM 4,5
BILHOES DE
REGISTROS NO
PRIMEIRO SEMESTRE

QUANDO COMPARADO AO MESMO PERIODO EM 2017, O NUMERO DE REGISTROS PERDIDOS, ROUBADOS OU COMPROMETIDOS AUMENTOU EM 133%; A SAUDE CONTINUA A LIDERAR EM NUMERO DE INCIDENTES (27%).

PORTAL SECURITY REPORT - 10/10/2018



#> ESTAMOS EXPOSTOS?



PESQUISADORES
DESCOBREM FALHAS
QUE PERMITEM
FALSIFICAR SINAIS
VITAIS DE PACIENTE

TIME DA MCAFEE DESCOBRIU UMA FRAQUEZA NO PROTOCOLO RWHAT USADO PELOS DISPOSITIVOS MEDICOS; SE UM HACKER EXPLORAR ESSA VULNERABILIDADE, ELE PODERA FORNECER INFORMACOES FALSAS A EQUIPE MEDICA EM TEMPO REAL

PORTAL SECURITY REPORT - 14/08/2018



#> ESTAMOS EXPOSTOS?



HACKERS VENDEM
DADOS DE 127
MILHOES DE CONTAS
NA DARK WEB

MAIS 127 MILHOES DE SENHAS DE OITO SITES SURGIRAM A VENDA NO DREAM MARKET, UM MERCADO DE PRODUTOS ILEGAIS QUE FUNCIONA NA DARK WEB. A DESCOBERTA FOI FEITA PELO SITE BRITANICO THE REGISTER, NA ULTIMA QUINTA-FEIRA (14), QUE RELATOU QUE PACOTE COMPLETO DE INFORMACOES ROUBADAS PODIA SER OBTIDO PELO EQUIVALENTE A R\$ 54 MIL EM BITCOIN.

PORTAL TECH TUDO - 16/02/2019



#> SEGURANCA OFENSIVA



VULNERABILITY MANAGEMENT IS A CORE
ELEMENT IN MODERN INFORMATION
TECHNOLOGY (IT) COMPLIANCE.



#> SEGURANCA OFENSIVA



CENARIO ATUAL



#> SEGURANCA OFENSIVA



WHEN CONSIDERING THE CYBERSECURITY LANDSCAPE, IT'S IMPORTANT TO NOTE THAT THE VERSIONS OF PRODUCTS THAT ORGANIZATIONS HAVE DEPLOYED EXIST ON A SPECTRUM, WITH A SMALL NUMBER OF ORGANIZATIONS RUNNING THE LATEST VERSIONS, MOST ORGANIZATIONS RUNNING OLDER BUT STILL SUPPORTED VERSIONS, AND A SUBSTANTIAL NUMBER OF ORGANIZATIONS RUNNING INFORMATION SYSTEMS THAT ARE NO LONGER SUPPORTED BY THE VENDOR.

[OPENVAS.ORG](https://openvas.org)



#> SEGURANCA OFENSIVA

RANSOMWARE WANNACRY

IT'S USUALLY THE ORGANIZATIONS RUNNING OUTDATED OR UNSUPPORTED PRODUCTS THAT YOU HEAR ABOUT WHEN A LARGE CYBERSECURITY INCIDENT OCCURS. FOR EXAMPLE, THE 2017 WANNACRY RANSOMWARE ATTACK DISPROPORTIONALLY IMPACTED ORGANIZATIONS THAT HAD SERVERS RUNNING THE WINDOWS SERVER 2003 OPERATING SYSTEM WHERE THE PORTS THAT ARE USED FOR SMB STORAGE PROTOCOL WERE EXPOSED TO THE INTERNET.

INF246X - ENTERPRISE SECURITY FUNDAMENTALS - EDX.ORG

#> \$ \$ \$ \$ \$



THE **COST** OF A BREACH IS ALWAYS AN **ESTIMATE**. EVEN AFTER A BREACH OCCURS, THE ACTUAL COST OF THE BREACH MAY NEVER BE ACCURATELY DETERMINED. ON TOP OF THE **DISRUPTION** TO THE **BUSINESSES PROCESSES**, IT IS DIFFICULT TO ASSESS THE VALUE OF **INTANGIBLES** SUCH AS **REPUTATIONAL** DAMAGE, THE COST OF **REHABILITATING** COMPROMISED SYSTEMS, THE COST OF **INVESTIGATING** THE BREACH ITSELF AND THE COST OF ANY FINES OR **PENALTIES** THAT MAY NEED TO BE PAID TO THE RELEVANT AUTHORITY.

INF246X - ENTERPRISE SECURITY FUNDAMENTALS - EDX.ORG



#> \$ \$ \$ \$ \$



O CUSTO DA *PREVENCAO* E SEMPRE
MENOR QUE O CUSTO DA *REMEDIACAO*.



THE ASSUME COMPROMISE **PHILOSOPHY** TAKES THE POSITION THAT AN ORGANIZATION SHOULD BUILD AND MAINTAIN ITS SECURITY POSTURE BASED ON THE IDEA THAT THE ORGANIZATION'S INFORMATION **SYSTEMS** HAVE ALREADY BEEN **COMPROMISED**.



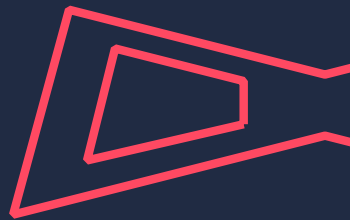
#> ETHICAL HACKER

UM HACKER ETICO E UM ESPECIALISTA EM SISTEMAS E REDES DE COMPUTADORES QUE CONHECE AS TECNICAS E METODOS UTILIZADOS PARA SE ENCONTRAR VULNERABILIDADES DE SEGURANCA EM SOFTWARES E REDES CORPORATIVAS.

[HTTP://PROFISSAOHACKER.COM/](http://PROFISSAOHACKER.COM/)

#> SEGURANCA OFENSIVA

HACKING
IS NOT A CRIME



#> SEGURANCA OFENSIVA



CERTIFICACOES



#> SEGURANCA OFENSIVA



RED TEAM



BLUE TEAM



#> SEGURANCA OFENSIVA



QUAL O DESAFIO QUE
TEMOS NAS EMPRESAS?



#> SEGURANCA OFENSIVA

A TECNOLOGIA NAO
INTERROMPE A AÇAO DE UM
HACKER.

LGPD

GDPR

A SEGURANÇA OFENSIVA FAZ PARTE DO SEU ESCOPO?

#> SEGURANCA OFENSIVA



"MAS NOS JA
INVESTIMOS 300 HORAS
DE PROJETO..."



#> SEGURANCA OFENSIVA

"ESTA EM FASE DE TESTES,
O FORNECEDOR NAO VAI
ARRUMAR, **VAMOS PUBLICAR**
MESMO ASSIM..."

#> SEGURANCA OFENSIVA

"NAO PODE ATUALIZAR, NOSSO SISTEMA FUNCIONA SOMENTE NESTA VERSAO..."

#> SEGURANCA OFENSIVA



"TUDO ISSO PARA
CONTROLAR O ACESSO
AO WIFI?"



DESAFIO 1

TRANSFORMAR A FRUSTACAO

EM MOTIVACAO.

#> SEGURANCA OFENSIVA

DESAFIO 2

COMO PODEMOS **MUDAR**

O CENARIO DAS **EMPRESAS?**

#> ENCERRAMENTO

A PERGUNTA NAO E "SE" VAMOS
SER INVADIDOS, MAS SIM
"QUANDO" SEREMOS.

#> ENCERRAMENTO



TUDO É UMA QUESTÃO DE
TEMPO, DINHEIRO E
OPORTUNIDADE.



#> ENCERRAMENTO

OBRIGADO



DEFCON



LET'S HACK